

## REMARKS

Claims 1-13 are pending in the application as originally filed. A first Office Action issued with all claims rejected under 35 USC §103(a) as being unpatentable over various combinations of prior art references including McCreery et al. (U.S. Patent No. 5,787,253), Henrick et al. (U.S. Patent No. 6,055,510), Reilly et al. (U.S. Patent No. 5,740,549), and Dobbins et al. (U.S. Patent No. 6,249,820). Applicants arguments resulted in the rejections being withdrawn and new grounds for rejection imposed in view of new art not previously cited by the Examiner.

Claims 1-13 have been rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,804,701 (Muret, et al.).

Because of clear differences between the Muret reference and the claimed elements of the current invention, no amendments are considered necessary for allowance over the prior art at issue and, consequently, no changes have been made to the claims. Accordingly, reconsideration and allowance of all claims is respectfully requested in view of the following remarks.

Two independent claims (1 and 9) are pending in the current application. The following remarks address the absence of certain features of these claims in the Muret patent. In particular:

A. Muret Fails to Teach the Step in Claim 1 of "Presetting IP Filters"

In addressing the claim 1 limitation calling for the step of "presetting IP filters," the Examiner refers to the following portion of Muret:

Log Parser Module (210)

FIG. 4 is a flowchart and schematic diagram illustrating a preferred control routine for the log parser module 210 of FIG. 3, configured to process static log files 510. One of the most time consuming operations is reading and processing the raw log files 510. With individual log files 510 containing potentially over a gigabyte of data, getting the raw data into the system 100 is an important step.

The purpose of the log parser module 210 is to efficiently read each log line 512 and separate it into its individual fields. The fields can include the IP address, timestamp, bytes sent, status code, referral, etc. As discussed above, each log line 512 in the log file 510 represents a hit or transaction from one of the web servers 500.

(Muret, col. 7, lines 58 through col. 8, line 3)

The above text only states that the IP address of the visitor computer can be a field in the log file stored at the web server. IP filters are not mentioned in Muret. In fact, the word "filter" occurs only once in Muret [col. 6, line 67] and only then refers to website identification by use of regular expression filters. The remainder of the Muret application references three methods for obtaining the visitor IP address, including (1) a web server

logging the IP address of the visitor, (2) using DNS to resolve the host and domain information, or (3) using a DNS Resolver Module (260) operable on the Muret web traffic analyzer 100. [see, e.g., col. 13, lines 19-57] None of the methods for resolving the IP address involve setting filters.

Even more importantly, there is no reference or suggestion within Muret that IP filters should be preset. In the present application, the invention addresses the problem of discounting irrelevant visitors to a particular web site (e.g. from the company's own computers) when establishing pertinent traffic data. This problem is stated in the specification of the present application at page 2, lines 4-10.

Muret does not address the problem with IP filtering, does not present a solution for web filtering, and in fact does not appear to even allow a preset filter to be incorporated within the data analyzing tool used to parse the data and provide a web traffic report. Any parse function that could be applied to the web log data to display IP addresses of visitors to specific web sites under Muret would have to be enacted after the data is collected. There is no function recited within Muret that would allow a filter on the IP data to be implemented prior to collection of the data (e.g. "presetting...").

Rejection of pending claims under 35 USC §102(e) would therefore be inappropriate in this case.

**B. Muret Fails to Teach the Step in Claim 1 of Storing a Web Page Including "Data Mining Code"**

In addressing the claim 1 limitation calling for the step of storing a web page on a first server where the web page includes "data mining code," the Examiner refers to the following portion of Muret:

Extremely busy websites will often use an array of servers to handle the extreme load of traffic. Other websites may have a secure server area that resides on a special machine.

Whether for robustness or functionality, multiple server architecture is a common practice and appears to create a unique problem for internet traffic analysis and reporting. Each web server 500 will create its own log file 510, recording entries from visitors as they travel through the website. Often, a single visitor will create log entries in the log file 510 for each web server 500, especially if the web servers 500 perform different functions of the website.  
(Muret, col. 10, lines 58-67)

Muret operates by querying the web servers for log file data rather than receiving data directly from the visitor computers themselves via data mining code embedded within the web pages sent from the web servers. It is clear from the citation in Muret above that the web servers themselves create the log files from web page visits. There is no mention in Muret

that the web pages themselves served to the visitors would include data mining code that obtains this information. A more appropriate description of Muret is that the web server has stored thereon some sort of data mining code, but that the web pages it serves do not include such code.

Furthermore, as no data mining code is transferred with the Muret web page, the "operating the data mining code on the visitor computer" step cannot be performed. Since the Muret web pages do not include data mining code, these claim 1 limitations are not found in Muret and rejection under §102(e) would be inappropriate.

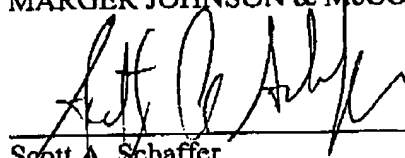
Claim 7 additionally includes a web site node operable to provide media content and data mining code to the visitor node. As data mining code is not provided to the visitor under the web server data record keeping of the Muret system, claim 7 would not be anticipated by Muret. Finally, claim 7 further requires a tracking node responsive to communication from a visitor node. The topography of the Muret system does not allow direct communication between the web site visitor and the data tracking system (100) as shown in Muret FIGs. 1 and 2. Accordingly, such an element is not shown in Muret and claim 7 should be allowable over the prior art of record.

#### CONCLUSION

For the foregoing reasons, reconsideration and allowance of claims 1-13 of the application as amended is solicited. The Examiner is encouraged to telephone the undersigned at (503) 222-3613 if it appears that an interview would be helpful in advancing the case.

Respectfully submitted,

MARGER JOHNSON & McCOLLOM, P.C.

  
\_\_\_\_\_  
Scott A. Schaffer  
Reg. No. 38,610

MARGER JOHNSON & McCOLLOM, P.C.  
210 SW Morrison St., Suite 400  
Portland, Oregon 97204  
Telephone: 503-222-3613  
Customer No. 20575